IN THE CLAIMS

1.   (Currently Amended)   A method of security enforcement for a persistent ~~computer~~ data repository comprising:

        intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items, the nonintrusive manner gathering the data access transaction from a stream of data between the application and the data repository;

        determining a correspondence of ~~if~~ the intercepted data access transaction ~~corresponds~~ to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access; and

        selectively limiting, based on the determined correspondence to the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items are modified in a resulting data access transaction according to the security policy, limiting the data access transaction further including:

                receiving a set of packets, the packets encapsulating the data access transaction according to layered protocols;

                interrogating and modifying the packets in a nondestructive manner with respect to the application layered protocols, the nondestructive manner preserving an expected application layer protocol encapsulation; ~~and~~

                padding the packets to emulate packets having a corresponding length as the restricted data items ~~for accommodating elimination of the restricted data items~~ to generate the resulting data access transaction in a manner preserving encapsulation according to expected application based layered protocols;

                identifying rows in the packets having restricted data items, and

~~eliminating the identified rows from the data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items, the resulting data access transaction returned to a requestor without restricted data items.~~

2.   (Original) The method of claim 1 wherein the security policy has rules, each of the rules including an object, a selection criteria and an action, the action indicative of restricted data items.

3.   (Original) The method of claim 1 wherein the data indications are references to data items in the data repository and limiting further includes qualifying the references to generate a modified request indicative of unrestricted data items, such that successive retrieval operations employing the qualified references do not retrieve restricted data items.

4.   (Original) The method of claim 3 wherein the data access transaction is a data access statement operative to request data and limiting further comprises:
        identifying at least one rule, according to the security policy, corresponding to the data access statement, the identified rule restricting access to at least one of the data items indicated by the data access statement; and
        concatenating selection qualifiers to the data access statement corresponding to the identified rule, the selection qualifiers operable to omit the restricted data items from the qualified references of the data access statement.

5.   (Currently Amended) The method of claim 1 wherein the data indications are rows of data retrieved from the data repository~~, and limiting further comprises:~~

~~identifying rows having restricted data items, and~~

~~eliminating the identified rows from the data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items.~~

6.   (Original) The method of claim 5 wherein the data access transaction is a data query response including a row set and limiting further comprises:

comparing each of the rows in the row set to the rules of the security policy; and

selectively eliminating rows in the row set including the restricted data items, based on the comparing, to generate a modified query response including a filtered row set.

7.   (Original) The method of claim 2 wherein the actions are selectively indicative of modifications, the modifications further comprising attributes, operators, and operands, the limiting further comprising

identifying data items corresponding to the attributes, each of the attributes associated with an operator and an operand;

applying an operator specified for the data item to the operand specified for the data item; and

determining, as a result of applying the operator, whether to eliminate the identified data item.

8.   (Original) The method of claim 1 wherein the nonintrusive manner is undetectable to the user application and undetectable to the data repository.

9.   (Canceled)

10.   (Canceled)

11.   (Previously Presented) The method of claim 1 wherein generating the resulting data access transaction preserves the encapsulating layered protocol associating the packets without employing a proxy for regenerating the sequence of packets.

12.   (Original) The method of claim 4 wherein intercepting the data access statement includes receiving an SQL query and limiting includes appending conditional selection statements to the SQL query, the conditional selection statements computed from the security policy, to generate the resulting data access transaction.

13.   (Original) The method of claim 12 further comprising:

building a parse tree corresponding to the SQL query;

adding nodes in the parse tree corresponding to the appended conditional selection statements; and

reprocessing the parse tree to generate the resulting data access transaction.

14.   (Original) The method of claim 6 wherein intercepting the data query response further comprises:

intercepting the data query response from the data repository as the data access transaction, the data query response encapsulated as a row set having rows from a relational database query, and further wherein limiting includes discarding rows in the row set having restricted data items and transmitting the remaining rows to the user as the resulting data access transaction.

15.   (Original) The method of claim 1 wherein the nonintrusive manner is such that the intercepting and limiting occurs undetectable to both the source and the destination of the data access transaction.

16.   (Original) The method of claim 1 wherein intercepting further comprises:

establishing an identification exchange intended for interception and operable to transmit an identification token indicative of an application user; and

parsing, as part of the intercepting, the identification exchange to extract the identification token, wherein the identification exchange is benign to the data repository.

17.   (Original) The method of claim 1 wherein intercepting occurs in a data path between a source of the data access transaction and a destination of the resulting data access transaction, and limiting occurs in a component separate from the source and destination.

18.   (Original) The method of claim 17 wherein the component separate from the source and destination is a separate network device than the components corresponding to the source and destination.

19.   (Original) The method of claim 1 wherein the restricted data items are eliminated from the resulting data access transaction.

20.   (Currently Amended) A method for nonintrusive implementation of ~~computer~~ data level security enforcement comprising:

defining a security policy between an application and a data repository, the security policy having rules indicative of restricted data items, the rules associated with attributes and conditions;

identifying an entry point between the data repository and the application;

deploying a security filter at the entry point, the security filter operable to receive data manipulation messages between the application and the data repository; the security filter further operable to limit data exposure by the data repository by selectively modifying the data manipulation messages into conformance with the security policy, the limiting further comprising:

sniffing the entry point to determine data manipulation messages;

intercepting the sniffed data manipulation messages in a nondestructive manner with respect to the layered protocols, the nonintrusive manner gathering the data access transaction from a stream of data between the application and the data repository, the nondestructive manner preserving expected application based layered protocols;

comparing the sniffed messages to the rules in the security policy and determine if the sniffed data manipulation message include restricted data items;

determining ~~if the sniffed messages~~ a match between the sniffed messages and at least one of the rules of the security policy;

selectively modifying, based on the determined match ~~if the determining indicates a~~ between the rules and the data manipulating message, the data manipulation message to remove the matching restricted data item, modifying further including:

building a parse tree corresponding to the SQL query;

adding nodes in the parse tree corresponding to the appended conditional selection statements; and

reprocessing the parse tree to generate the resulting data access transaction in a manner preserving encapsulation according to expected application based layered protocols, the resulting data access transaction returned to a requestor without restricted data items.

21.   (Original) The method of claim 20 wherein determining comprises comparing attributes of the data manipulation messages with operators and operands in the compared rules, the operators and operands indicative of restricted data items in the data repository.

22.   (Original) The method of claim 20 wherein modifying further comprises:

reconstructing a request query corresponding to a query syntax; and

adding limiters to the request query corresponding to the matching rules of

the security policy, the adding performed in a nondestructive manner such that

the modification is undetectable to the data repository.

23.   (Original) The method of claim 20 wherein modifying further comprises:

identifying a data retrieval response encapsulated in a layered protocol on

the data manipulation message; and

reconstructing the data retrieval response by deleting restricted data items

from the data retrieval response, the reconstructing performed in a

nondestructive manner undetectable to the application and conforming to the

encapsulating layered protocol.

24.   (Currently Amended) A computer data security filter device for security

enforcement for a persistent data repository comprising:

an interceptor in the security filter operable to intercept, in a nonintrusive

manner, a data access transaction between a user application and a data

repository having data items, the nonintrusive manner gathering the data access

transaction from a stream of data between the application and the data

repository;

a security policy table responsive to the interceptor to determine a

correspondence of if the intercepted data access transaction corresponds to the

security policy table, the security policy table indicative of restricted data items in

the data repository to which the user application is prohibited access; and

a limiter operable to selectively limit, based on the determined

correspondence to the security policy, the data access transaction by modifying

the data access transaction such that data indications, in the data access

transaction, and corresponding to restricted data items, according to the security

policy table, are modified in a resulting data access transaction, the security filter

operable to manipulate the resulting data access transaction in a nonintrusive manner such that modifications performed on the data access transaction are undetectable to the user application and undetectable to the data repository, the data access transaction being contained in a set of packets, the limiter further operable to:

receive the set of packets, the packets encapsulating the data access transaction according to application based layered protocols; and

interrogate and modify the packets in a nondestructive manner with respect to the layered protocols, the nondestructive manner preserving expected application based layered protocols;

pad the packets to emulate packets having a corresponding length as the restricted data items to generate the resulting data access transaction in a manner preserving encapsulation according to expected application based layered protocols;

identify rows in the packets having restricted data items; and

eliminate the identified rows from the data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items, the resulting data access transaction returned to a requestor without restricted data items.

25.   (Original) The security filter of claim 24 wherein the security policy has table rules, each of the rules including an object, a selection criteria and an action, the action indicative of restricted data items.

26.   (Original) The security filter of claim 24 wherein the data indications are references to data items in the data repository and the limiter is operable to qualifying the references to generate a modified request indicative of unrestricted data items, such that successive retrieval operations, from the data repository, employing the qualified references do not retrieve restricted data items.

27.   (Original) The security filter of claim 26 wherein the data access transaction is a data access statement operative to request data, wherein:

the interceptor is operable identify at least one rule, according to the security policy, corresponding to the data access statement, the identified rule restricting access to at least one of the data items indicated by the data access statement; and

the limiter is operable to concatenate selection qualifiers to the data access statement corresponding to the identified rule, the selection qualifiers operable to omit the restricted data items from the qualified references of the data access statement.

28.   (Original) The security filter of claim 24 wherein the data indications are rows of data retrieved from the data repository, wherein:

the interceptor is operable to identify rows having restricted data items, and

the limiter is operable to eliminate the identified rows from the data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items.

29.   (Original) The security filter of claim 28 wherein the data access transaction is a data query response including a row set wherein:

the interceptor is operable to compare each of the rows in the row set to the rules of the security policy; and

the limiter is operable to selectively eliminate rows in the row set including the restricted data items, based on the comparing, to generate a modified query response containing a filtered row set.

30.   (Original) The security filter of claim 25 wherein the actions are selectively indicative of modifications, the modifications further comprising attributes, operators, and operands, wherein the limiter is operable to:

identify data items corresponding to the attributes, each of the attributes associated with an operator and an operand;

apply an operator specified for the data item to the operand specified for the data item; and

determine, as a result of applying the operator, whether to eliminate the identified data item.

31.   (Canceled)

32.   (Canceled)

33.   (Original) The security filter of claim 24 wherein the data access transaction is contained in a set of packets wherein the limiter is operable to:

receive the set of packets, the packets encapsulating the data access transaction according to layered protocols;

interrogate and modify the packets in a nondestructive manner with respect to the layered protocols; and

pad the packets for accommodating elimination of the restricted data items to generate the resulting data access transaction.

34.   (Original) The security filter of claim 33 wherein the resulting data access transaction conforms to the encapsulating layered protocol associating the packets.

35.   (Original) The security filter of claim 27 wherein the data access statement is an SQL query and wherein the limiter is operable to append conditional selection statements to the SQL query, the conditional selection statements computed from the security policy, to generate the resulting data access transaction.

36.   (Original) The security filter of claim 35 further comprising a parse tree, the interceptor operable to build the parse tree corresponding to the SQL query, wherein the limiter is further operable to add nodes to the parse tree corresponding to the appended conditional selection statements; and reprocessing the parse tree to generate the resulting data access transaction.

37.   (Original) The security filter of claim 24 wherein the interceptor is operable to intercept the data query response from the data repository as the data access transaction, the data query response encapsulated as a row set having rows from a relational database query, wherein the limiter is operable to discard rows in the row set having restricted data items and transmit the remaining rows to the user as the resulting data access transaction.

38.   (Original) The security filter of claim 24 wherein the user application and the data repository define a data path between a source of the data access transaction and a destination of the resulting data access transaction, wherein the security filter is disposed in a component separate from the source and destination.

39.   (Original) The security filter of claim 38 wherein the component separate from the source and destination is a separate network device than the components corresponding to the source and destination

40.   (Currently Amended) A method for nonintrusive implementation of computer data level security enforcement comprising:

    defining a security policy having rules, the rules further specifying attributes and conditions;

    intercepting a data retrieval request in a nonintrusive manner, the nonintrusive manner gathering the data access transaction from a stream of data between an application and a data repository;

comparing the data retrieval request to the security policy;

determining a correspondence between~~if~~ the data retrieval request ~~and~~~~corresponds to~~ at least one of the rules of the security policy;

identifying, via a parse tree, selectivity operators indicative of the data to be retrieved;

selectively modifying, based on the determined correspondence, the parse tree according to the corresponding rule to generate a modified data retrieval request; and

forwarding the modified data retrieval request to the data repository for subsequent retrieval and transport to the requesting user, modifying the parse tree further including

building a parse tree corresponding to the SQL query;

adding nodes in the parse tree corresponding to the appended conditional selection statements; and

reprocessing the parse tree to generate the resulting data access transaction by modifying the packet content being delivered to the database consistent with the original data retrieval request, the generated resulting data access transaction preserving encapsulation according to application based layered protocols expected in the original data retrieval request, the resulting data access transaction returned to a requestor without restricted data items.

41.   (Currently Amended) A computer program product having a computer readable storage medium operable to store computer program logic embodied in computer program code including a set of instructions responsive to a processor encoded thereon that, when executed by the processor, cause the computer to perform a method of~~for~~ implementing security enforcement in a persistent data repository comprising:

computer program code for intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data

items; the nonintrusive manner gathering the data access transaction from a stream of data between an application and a data repository:

computer program code for determining if the intercepted data access transaction corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access; and

computer program code for limiting, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, and corresponding to restricted data items are modified in a resulting data access transaction according to the security policy, intercepting the data access statement including receiving an SQL query and limiting including appending conditional selection statements to the SQL query, the conditional selection statements computed from the security policy, to generate the resulting data access transaction, further comprising:

computer program code for building a parse tree corresponding to the SQL query;

computer program code for adding nodes in the parse tree corresponding to the appended conditional selection statements; and

computer program code for reprocessing the parse tree to generate the resulting data access transaction, the generated resulting data access transaction preserving encapsulation according to application based layered protocols expected in the original data retrieval request, the resulting data access transaction returned to a requestor without restricted data items.

42.   (Currently Amended) A computer readable storage medium operable to store computer program logic embodied in computer program code including a set of instructions responsive to a processor encoded thereon that, when executed by the processor, cause the computer to perform a method of for security enforcement for a persistent data repository comprising:

program code for intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items, the nonintrusive manner gathering the data access transaction from a stream of data between the application and the data repository;

program code for determining a correspondence of if the intercepted data access transaction corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access; and

program code for selectively limiting, based on the determined correspondence to the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy, are modified in a resulting data access transaction, intercepting occurring in a data path between a source of the data access transaction and a destination of the resulting data access transaction, and limiting occurring in a component separate from the source and destination, the component separate from the source and destination being a distinct network device from the components corresponding to the source and destination such that the nonintrusive manner is undetectable to the user application and undetectable to the data repository by preserving encapsulation according to expected application based layered protocols in the resulting data access transaction, limiting the data access transaction further including:

receiving a set of packets, the packets encapsulating the data access transaction according to layered protocols;

interrogating and modifying the packets in a nondestructive manner with respect to the application layered protocols, the nondestructive manner preserving an expected application layer protocol encapsulation;

padding the packets to emulate packets having a corresponding length as the restricted data items to generate the resulting data access

transaction in a manner preserving encapsulation according to expected application based layered protocols;

identifying rows in the packets having restricted data items, and eliminating the identified rows from the data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items, the resulting data access transaction returned to a requestor without restricted data items.

43.   (Currently Amended) A data security filter device for security enforcement for a persistent data repository comprising:

means for intercepting, in a nonintrusive manner, a data access transaction between a user application and a data repository having data items, the nonintrusive manner being undetectable to the user application and undetectable to the data repository, the nonintrusive manner gathering the data access transaction from a stream of data between the application and the data repository;

means for determining a correspondence ofif the intercepted data access transaction-corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access; and

means for selectively limiting, based on the determined correspondence to the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy, are modified in a resulting data access transaction;

the data indications being rows of data retrieved from the data repository, such that the means for limiting further comprises:

means for receiving a set of packets, the packets encapsulating the data access transaction according to layered protocols;

means for interrogating and modifying the packets in a nondestructive manner with respect to the layered protocols the nondestructive manner preserving expected application based layered protocols;

means for identifying rows having restricted data items;

means for eliminating the identified rows from the data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items;

means for padding the packets to emulate packets having a corresponding length as the restricted data items for accommodating elimination of the restricted data items to generate the resulting data access transaction, generating the resulting data access transaction preserving the encapsulating layered protocol associating the packets without employing a proxy for regenerating the sequence of packets;

the data access transaction being a data query response including a row set such that the means for limiting further includes:

means for comparing each of the rows in the row set to the rules of the security policy; and

means for identifying rows in the packets having restricted data items, and

means for selectively eliminating rows in the row set including the restricted data items, based on the comparing, to generate a modified query response including a filtered row set corresponding to packets expected according to application based layered protocols of the intercepted data access transaction such that the resulting data access transaction is a modified query response including rows without restricted data items, the resulting data access transaction returned to a requestor without restricted data items.

44.   (Previously Presented) The method of claim 1 wherein the nonintrusive manner is undetectable to the user application and undetectable to the data

repository, the nonintrusive manner such that the intercepting and limiting occurs undetectable to both the source and the destination of the data access transaction, wherein intercepting occurs in a data path between a source of the data access transaction and a destination of the resulting data access transaction, and limiting occurs in a component separate from the source and destination, and the component separate from the source and destination is a separate network device than the components corresponding to the source and destination.

45.   (Previously Presented)   The method of claim 1 wherein padding the packet further comprises nondestructively modifying the packet such that the packet appears undisturbed to the receiver.

46.   (Previously Presented) The method of claim 1 wherein modifying further comprises:

        nondestructively modifying a payload of the packet at the application layer; and

        leaving encapsulated, non-payload control information in the packet undisturbed.